УДК 004

# ЗБЕРІГАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ ТА ВАЖЛИВИХ ДАНИХ ДЛЯ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У МОБІЛЬНИХ ЗАСТОСУНКАХ В АВТОМОБІЛЬНІЙ БЕЗПЕЦІ

О. Ю. Конорєв[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

## Анотація

Робота присвячена проблемі безпечного зберігання таємних ключів та чутливої інформації користувачів, яка використовується для автентифікації користувача в сервісі для віддаленного керування розумним автомобілем за допомогою застосунка на мобільному пристрої. В роботі запропоновано безпечний метод зберігання таємниці на мобільному пристрої користувача, який відрізняється використанням довіреного середовища виконання.

*Ключові слова*: інформаційна безпека, розумні автомобілі, довірене середовище виконання.

## Вступ

Сучасні автомобільні компанії випускають велику кількість автомобільних новинок, приділяючи велику увагу технічним питанням безпеки, однак, питанням інформаційної безпеки досі не приділяється належної уваги. Про це свідчать дослідження, проведені в роботах[1, 2, 3, 6, 5]. Причинами такої неуважності, як правило є: недооцінка можливостей використання бортової інформаційної системи автомобіля зловмисниками, відсутність єдиного безпечного циклу розробки програмно-апаратних складових інформаційної системи автомобіля, коли питанням безпеки приділяється належна увага починаючи із процесу проектування і до процесу впровадження продукту. Питання усунення вразливостей, притаманних протоколам обробки інформації в інформаційній системі автомобіля та застосункам, які беруть участь в організації взаємодії "користувач - інформаційная система автомобіля", досі залишаються актуальними. В даній роботі виконано аналіз загроз для бортової інформаційної системи та її взаємодії із зовнішніми системами. Виділено загрози, які спрямовані на ключі, що використовуються при автентифікації користувача (і відповідного застосунка) сервісом керування інформаційною системою автомобіля. Запропоновано рішення, яке може використовуватись в цій сфері, розроблено програмне забезпечення, яке демонструє працездатність запропонованого рішення.

## 1. Особливості архітектури розумного авто

Обчислювальні та комунікаційні системи все більш використовуються і безперервно розвиваються. Комп'ютеризація впроваджується до всіх сфер життя людини, в тому числі й до автомобільної індустрії. До недавнього часу автомобілі контролювалися виключно механічними засобами, але, завдяки комп'ютеризації, автомобілі наділяються вбудованими компютерними системами, електронними блоками, процесорами. Сучасний автомобіль може в собі містити більш ніж 80 електронних блоків, які взаємодіють один з одним за допомогою внутрішньої мережі автомобіля, а в деяких випадках – за допомогою бездротових технологій. Електронні блоки обмінюються інформацією між собою, використовуючи комунікаційні мережі CAN [9] , LIN [7], FlexRay [8] тощо. Також в кожному сучасному автомобілі є OBD–II порт, який використовується для діагностики автомобіля. Використовуючи його, можна підлкючится до CAN–шини.

Електронні блоки відповідають за різні задачі, починаючи від закриття дверей або активування склопідйомників і закінчуючи гальмівною системою автомобіля. Виведення з ладу одного з блоків може призвести до серйозних проблем для водія та його пасажирів.

Останнім часом автовиробники почали наділяти свої автомобілі інформаційно–розважальними (англ. infotainment) та телематичними (англ. telematic) системами. Інформаційно-розважальна система об'єднує апаратне і програмне забезпечення і пропонує користувачу розважальні функції, включаючи: GPS-навігацію, плеєр, SMS, USB, Bluetooth, Hands-free дзвінки, Wi–Fi, мобільний інтернет. Телематична система, на відміну від Інформаційно–розважальної, не включає в себе розважальні функції. Такі розробники, як Kia, Lexus, BMW навіть обє'днуть infotainment і telematics системи в одну – Kia Uvo, Lexus Enform, BMW ConnectedDrive. Функції, які зазвичай зустрічаються в системі телематики автомобіля: віддалений доступ, GPS, контроль швидкості авто, екстренні виклики, діагностика авто.

## 2. Джерела загроз та типові вразливості

Завдяки функціоналу, який надан інформаційно–розважальною та телематичною системами у власника автомобіля є можливість керувати своїм авто за допомогою застосунка на своєму мобільному пристрої. Наприклад, користувач може віддалено підключитися зі свого смартфона, використовуючи мобільний застосунок, до інформаційної системи авто й відкривати двері авто, вмикати двигун тощо. Компрометація одного з цих компонентів може призвести до втручання зловмисника в керування автомобілем. Наприклад, зловмисник здатен скомпрометувати інформаційно-розважальну систему автомобіля, використовуючи зловмисне ПО, і через це отримати доступ до CAN–шини, а далі отримати контроль над авто. Наприклад, посилаючи модулю, відповідному за гальмівну систему, зловмисно сформовані повідомлення. За останній час було проведено декілька досліджень [1, 2, 5, 6] в області безпеки автомобілей і спеціалісти демонстрували ряд вразливостей в автомобільних інформаційних системах.

Атаки на інформаційну систему автомобіля можно поділити на внутрішні та зовнішні. Для виконання внутршніх атак, зловмисник повинен мати фізичний доступ до автомобіля. Для виконання віддалених атак, зловмиснику потрібно використовувати бездротові технології. Виходячи з цього можна побудувати модель загроз 1 для інформаційної системи автомобіля. Основними початковими напрямками атак на інформаційну система автомобіля для зловмисника, який має фізичний доступ до авто є: OBD–II порт, USB–порт, CD/DVD плеєр.

OBD–II порт забезпечує прямий доступ до CAN-шини, і цього може бути достатньо для того, щоб скомпрометувати весь обсяг автомобільних систем; варто лише підключити спеціальний діагностуючий прилад до порта, цей прилад можно легко придбати [10]. Маючи фізичний доступ до OBD-II порта, зловмисник здатен:

- Встановити шкідливий діагностичний пристрій для відправки пакетів по CAN шині,
- Підключити до CAN-шини, щоб завантажити шкідливе ПО,
- Встановити шкідливий діагностичний пристрій для відстеження автомобіля,

Іншим напрямком є атака, яка починається з компрометації інформаційно-розважальної системи. Ця система може включає в себе USB–порт, CD/DVD плеєр. Практично всі автомобілі забезпечені програвачами компакт-дисків. Виробники автомобілів також забезпечують свої авто цифровими мультимедійний портами (USB–порт) для розширення можливостей мультімедійної системи автомобіля.

Отже, в зловмисника є кілька напрямків для здійснення атаки на систему. По–перше, зловмисник може загрузити компакт-диск зі шкідливим змістом, який шляхом кодування може бути представлений у вигляді композиції. Декодуючи дану композицію, програвач може бути скомпрометований. По–друге, зловмисник може підключити мобільний пристрій

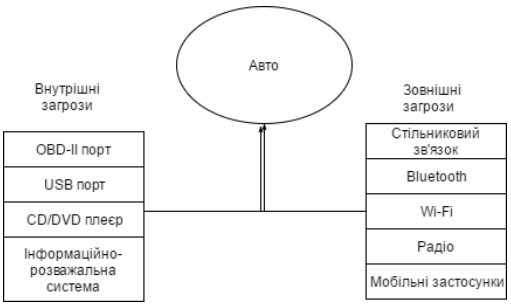


Рис. 1. Модель загроз

до USB-порту. Даний пристрій може мати зловмисне програмне забезпечення, виконання якого компрометує інформаційну систему авто.

Початковим напрямком віддалених атак на автомобіль можуть бути: Bluetooth, Wi–Fi, стільниковий зв'язок, радіо, мобільні застосунки. Bluetooth дозволяє користувачам підключати свій мобільний пристрій до інформаційної системи автомобіля. Підключивши мобільний пристрій, користувач може відповідати на дзвінки або переглядати SMS.

Експерти з інформаційної [6] безпеки знайшли вразливості у реалізації протоколу Bluetooth в інформаційній системі випробуваного ними авто. В даній реалізації протоколу Bluetooth використовувалось багато викликів вразливої функції strcpy, яка вразлива до атак переповнення буферу. Дослідники визначили, що пристрої, які під'єднані до інформаційно-розважальної системи за допомогою Bluetooth, здатні експлуатувати цю вразливість й виконувати свій зловмисний код у модулі, якій відповідає за Bluetooth.

Інформаційно-розважальна система також може мати Wi–Fi модуль. Користувачі можуть використовувати його для онлайн перегляду фільмів, оновлення програмого забезпечення тощо. Компрометація його може призвести до того, що зловмисник буде здатен отримати доступ до мережі автомобіля з великої відстані (приблизно 25-30 метрів) та оновити програмне забезпечення інформаційно-розважальної системи на зловмисне.

Напркилад, зловмисник здатен встановити підроблену точку доступу Wi–Fi з рекламою, яка пропонує користувачу оновити програмне забезпечення інформаційно-розважальної системи, яке в свою чергу є зловмисним. Реальним прикладом вразливої програмної реалізації Wi-Fi [1]. Можно зробити висновок, що основною вразливістю в даних інтерфейсах є небезпечна програмна реалізація. Про вразливості стільникового зв'язку та радіо можно дізнатись за посиланням [1, 6].

У подальшому в цій роботі буде розглядатися напрямок атак, пов'язанний з мобільними застосунками. Технологію віддаленного управління автомобілем підтримують багато автовиробників, серед них BWM, Tesla, Kia, Hyundai та ін. Користувачу достатньо завантажити застосунок на свій смартфон, зареєструвати свій обліковий запис на сайті компанії вирбоника застосунка, авторизуватися в мобільному

застосунку і після цього можна почати використовувати його.

Керування здійснюється віддалено, зазвичай, за допомогою CDMA зв'язку. Типовими вразливостями в мобільних застосунках, окрім вразливостей, пов'язаних з використанням небезпечних функцій мов програмування, є [2, 3, 5]: нешифрований трафік та небезпечне зберігання криптографічних ключів. Реальні приклади небезпечної реалізації застосунків.

Приклад 1: Мобільний застосунок Hyundai Blue Link [5]. Спеціалістам компанії Rapid7 вдалось виявити серйозні вразливості в даному застосунку. В цьому застосунку трафік пересилався за допомогою HTTP протоколу. Хоч і було присутнє сметричне шифрування, але криптографічний ключ зберігавсе небезпечно. Його можно було легко витягти з програми. Ключ був єдиним для всіх користувачів і його не можно було змінити. Зловмиснику залишалось перехопити дані, передані застосунком й розшифрувати ключем, який є однаковим для всіх користувачів.

Приклад 2: Застосунок компанії Tesla [2]. Під час установки цього застосунку власник повинен зареєструвати свій обліковий запис й запустити застосунок під своїм обліковим записом, який використовується для генерації OAuth токену. Іншим разом, коли користувач буде запускати цей застосунок, замість облікових даних буде використовуватися цей токен, який зберігається 90 днів. Дослідники [2] виявили, що застосунок Tesla зберігає цей токен в незашифрованому форматі. Атакуючий здатен створити шкідливий застосунок, який допоможе підвищити привілеї, а потім зможе прочитати або видалити цей токен. Якщо застосунок видалить токен, то користувачеві доведеться знову ввести свої облікові дані, які атакуючий може перехопити. Маючи облікові дані й токен, зловмисник здатен завести двигун авто, відчинити двері тощо. З цього можно зробити висновок, що основними загрозами ключам та токенам є невірна реалізація програмного забезпечення, нехтування або невірне використання засобів захисту інформації.

## 3. Рішення щодо безпечного зберігання таємниці

В даній роботі запропоноване рішення безпечного зберігання криптографічних ключів та важливих даних для автентифікації користувачів у мобільних застосунках. Дане рішення базується на використанні довіреного середовища виконання (англ. Trusted Execution Environment, TEE) [4]. Даний метод здатний ускладнити або зовсім усунути можливість проведення атак наведених в прикладах у розділі "Джерела загроз та типові вразливості".

TEE - це безпечне середовище виконання в процесорі. Процесор може працювати в звичайному (нормальне середовище, англ. Rich OS) або захищеному (безпечне середовище, англ. Trusted OS) режимах. Дана технологія забезпечує захищене зберігання даних, безпечне завантаження операційної системи, ізольоване виконання коду, шифрування даних тощо.

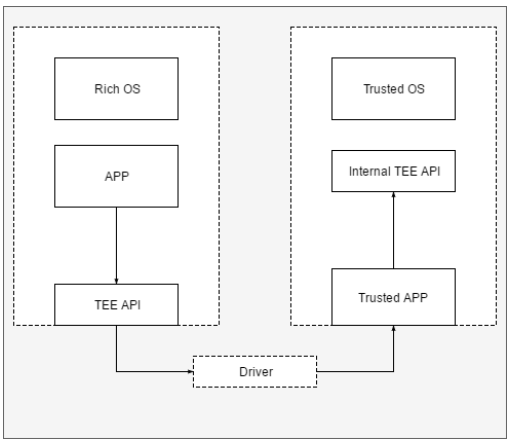


Рис. 2. Схема взаємодії між Rich OS та Trusted OS

Для того, щоб застосунок з нормального середовища мав здатність звертатися до сервісів, які надає TEE, він повинен використовувати інтерфейс програмування застосунків (англ. API) TEE. Програмне забезпечення, яке працює в звичайному режимі процесора, може використовувати API для підключення до довірених застосунків й відправляти запити на виконная певного функціоналу, який надає API.

Довірені застосунки виконуються в захищеній частині процесора й надають певний інтерфейс для роботи з TEE для застосунків із нормального середовища. За запитом застосунка із нормального середовища для використання функціоналу із безпечного, процесор перемикається в захищений режим для виконання відповідного функціоналу, який запросив застосунок із нормального середовища (рис. 2).

Для безпечного зберігання криптографічних ключів, генерації секретних токенів та важливих даних для аутентифікації користувачів потрібно реалізувати два застосунки: перший буде виконуватися в звичайному режимі процесора та взаємодіяти з другим застосунком, який буде виконуватися в захищеному режимі та безпечно надавати функціонал TEE.

Криптографічні ключі, які необхідні для шифрування трафіку, який надсилається серверу для виконання певного функціоналу над автомобілем необхідно зберігати у захищеній частині процесору. Для цього потрібно реалізувати довірений застосунок, який буде використовувати інтерфейс TEE для отримання криптографічних ключів від застосунка із нормального середовища та зберігати його в залежності від конфігурації, тобто дані можуть зберігатися як в безпечному середовищі, так і в нормальному. Якщо дані зберігаються в нормальному середовищі, то ці дані шифруються і них накладаються обмеження у доступі. Переваги запропонованого рішення - безпечне зберігання даних.

Порівнюючи з прикладами 1 та 2 з розділу "Джерела загроз та типові вразливості даний метод відрізняється саме безпечним зберіганням секретного ключа та токена. Тобто ніякі сторонні застосунки не будуть здатні отримати збережені дані, оскільки лише авторізовані застосунки будуть мати доступ до даних, що захищаються. На відміну від звичайного шифрування даних і зберігання їх в пам'яті, в дано-

му методі не потрібно турбуватися про зберігання ключа, яким шифруються ці дані.

## Висновки

В результаті роботи було проаналізовано основні вразливості інформаційній системі авто, а також визначені основі загрози ключам та даним, що використовуються для автентифікації користувача. Це виявилися невірна реалізація програмного забезпечення, неврніе використання або нехтування засобів захисту інформації. Також було розроблено застосунок, який демонструє працездатність запропонованого метода. Практична цінність роботи полягає в тому, що результати роботи можуть бути застосовані в розробці мобільних застосунків для керування автомобілем дистанційно, а також розповсюджені й на інші області управління розумними речами із використанням мобільного застосунку власника.

## Перелік використаних джерел


1. Chris Valasek, Charlie Miller- Remote Exploitation of an Unaltered Passenger Vehicle - Access mode: http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf.
2. Promon -Tesla cars can be stolen by hacking the app - Access mode: https://promon.co/blog/tesla-cars-can-be-stolen-by-hacking-the-app/.
3. - Security vulnerabilities in BMW's ConnectedDrive - Access mode: https://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html.
4. GlobalPlatform-Trusted Execution Environment- Access mode: https://www.globalplatform.org/mediaguidetee.asp.
5. Rapid 7-Security vulnerabilities in Hyundai Blue Link- Access mode: https://community.rapid7.com/community/infosec/blog/2017/04/25/r7-2017-02-hyundai-blue-link-potential-info-disclosure-fixed.
6. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno-Comprehensive Experimental Analyses of Automotive Attack Surfaces- Access mode: http://www.autosec.org/pubs/cars-usenixsec2011.pdfp.
7. ISO 17987-1:2016-Road vehicles – Local Interconnect Network (LIN)- Access mode: https://www.iso.org/standard/61222.html.
8. ISO 17458-1:2013-Road vehicles – FlexRay communications system- Access mode: https://www.iso.org/standard/59804.html.
9. ISO 11898-1:2015-Road vehicles – Controller area network (CAN)- Access mode: https://www.iso.org/standard/63648.html.
10. ISO 11898-1:2015-10 Best OBD2 Scanners- Access mode: https://wiki.ezvid.com/best-obd2-scannersl.